UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/654,417	09/04/2003	Philip Kwan	FOUND-0058 (034103-049)	7628

49680 7590 02/27/2009

FOUNDRY-NIXON PEABODY LLP
200 Page Mill Road
Palo Alto, CA 94306

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	**PAPER NUMBER**
2436	
MAIL DATE	**DELIVERY MODE**
02/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/654,417	KWAN ET AL.	
	Examiner	Art Unit	
	SHANTO M. ABEDIN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the communication filed on 12/01/2008.

2. Claims 1-46 have been presented for examination.

3. Claims 1-46 have been rejected.

Response to Arguments

4. The applicant's arguments regarding objections to the claims are fully considered,

5. The applicant's arguments regarding 35 USC 101 type rejections fully considered, however, found not persuasive. The applicant argues that the software implementation requires processing device to execute the software instructions. However, no such processing device or hardware is disclosed as a part of the claimed device or apparatus. Therefore, the claimed device or apparatus is considered to be software implemented device or apparatus since switch and ports can be implemented in software alone, and consequently being non statutory. The previous 35 USC 101 type rejections are maintained (please see the office action below for detail).

6. The applicant's arguments regarding the previous 35 USC 103(a) type rejections are fully considered, however, moot in view of new grounds of rejections presented in this office action.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-12, 35, 38-39 and 44 are rejected under 35 USC 101 since the claimed invention is directed to non-statutory subject matter.

Regarding claims 1 and 38, they are directed to a layer 2 access device, or an apparatus comprising ports, switching fabric, and control logic, however, according to the specification (Fig 2; Par 0044), these claimed features or components can be optionally implemented in software alone. In particular, claimed ports, switch, control logic can be implemented in software alone, and claimed apparatus, or access device lacks any processing device, or hardware or computer component that is necessary for falling within a statutory category of invention, and considered to be non-statutory. See MPEP 2106.01.

Regarding claims 2-12, 35, 39 and 44, they are rejected because of their dependencies on claims 1 or 38, and since they further fail to incorporate any computer hardware to the claimed apparatus or device.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-34 and 44-46 are rejected under 35 U.S.C. 102(e) as anticipated by Tsuchiya et al (US 7360086 B1) or, in the alternative, under 35 U.S.C. 103(a) as obvious over Kameda (US 2003/0028808 A1)

Regarding claim 1, Tsuchiya et al teaches network access device for providing network security, comprising:

a plurality of input ports (Fig 1.21-25; Col 1, starts at line 25; LAN switch with plural ports);

a switching fabric (Fig 1.11; switch) for routing data received on the plurality of input ports to at least one output port (Fig 7.210; LAN switch with the routing, and port information) and

control logic (Col 2, starts at line 35; Col 7, starts at line 5; authentication, or control information) adapted to authenticate a physical address of a user device coupled to one of the plurality of input ports (Col 8, starts at line 5; MAC address authentication), to authenticate user information provided by a user of the user device only if the physical address is valid (Fig 4, steps 102 and 103; Col 8, starts at line 5; Col 14, lines 10-59; authenticating user/source using the authentication table after matching/ checking the MAC address in the host table) , and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid (Fig 3; Fig 7; Col 2, lines 32-55;Col 14, lines 40-60; restricting port access based on control, or authentication table)

Alternatively, if the position for the inherency is not found supportable Kameda teaches control logic to authenticate user information provided by a user of the user device only if the physical address is valid (Fig 3, steps S32 and S33; Par 037, 038, 053, 54; authenticating the user once MAC address is authenticated) , and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid (Fig 1.2 and 51; Par 53-54, 60-62; assigning/ filtering ports according to the authentication database)

Kameda and Tsuchiya et al are analogous art because they are from the same field of endeavor of secure network communication. Therefore, at the time of invention, it would have

been obvious to a person of ordinary skill in the art to modify Tsuchiya et al 's authentication mechanism with the teachings of Kameda to design a device wherein network security/ access device wherein authenticate user information provided by a user of the user device only if the physical address is valid with a reasonable degree of success in order to provide a robust communication control mechanism.

Regarding claim 12, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches a method for providing network security, comprising:

authenticating in a network access device a physical address of a user device coupled to a port of the network access device (Col 8, starts at line 5; MAC address authentication);

authenticating user information provided by a user of the user device to the network access device only if the physical address is valid (Fig 4, steps 102 and 103; Col 8, starts at line 5; Col 14, lines 10-59; authenticating user/source using the authentication table after matching/ checking the MAC address in the host table); and

restricting access to the port in accordance with a user policy associated with the user information only if the user information is valid (Fig 3; Fig 7; Col 2, lines 32-55;Col 14, lines 40-60; restricting port access based on control, or authentication table).

Alternatively, if the position for the inherency is not found supportable Kameda teaches authenticating user information provided by a user of the user device to the network access device only if the physical address is valid (Fig 3, steps S32, S33; Par 037, 038, 053, 54; authenticating the user once MAC address is authenticated) , and restricting access to the port in accordance with

a user policy associated with the user information only if the user information is valid (Fig 1.2 and 51; Par 53-54, 60-62; assigning/ filtering ports according to the authentication database).

Regarding claim 23, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches a network system, comprising:

a data communications network (Fig 1; VLAN);

network access device coupled to the data communications network (Fig 1; LAN Switch); and

a user device coupled to a port of the network access device (Fig 1; PC);

wherein the network access device is adapted to authenticate a physical address of the user device (Col 8, starts at line 5; MAC address authentication), to authenticate user information provided by a user of the user device only if the physical address is valid (Fig 4, steps 102 and 103; Col 8, starts at line 5; Col 14, lines 10-59; authenticating user/source using the authentication table after matching/ checking the MAC address in the host table), and to restrict access to the port in accordance with a user policy associated with the user information only if the user information is valid (Fig 3; Fig 7; Col 2, lines 32-55;Col 14, lines 40-60; restricting port access based on control, or authentication table).

Alternatively, if the position for the inherency is not found supportable Kameda teaches control logic to authenticate user information provided by a user of the user device only if the physical address is valid (Fig 4, steps 102 and 103; Col 8, starts at line 5; Col 14, lines 10-59; authenticating user/source using the authentication table after matching/ checking the MAC address in the host table) , and to restrict access to the one of the plurality of input ports in accordance with

a user policy associated with the user information only if the user information is valid (Fig 3; Fig 7; Col 2, lines 32-55;Col 14, lines 40-60; restricting port access based on control, or authentication table).

Regarding claim 2, Tsuchiya et al teaches the network access device wherein the physical address comprises a Media Access Control (MAC) address (Col 1, starts at line 25; MAC address).

Regarding claim 3, Tsuchiya et al teaches the network access device wherein the control logic is adapted to authenticate the user information (Fig 3; Col 2, starts at line 32). Tsuchiya et al fails to teach utilizing IEEE 802. lx protocol. However, examiner takes an official notice on that at the time of invention, use of IEEE 802. lx protocol in wireless/ VLAN security was well known in the art (see US 7188364 B2). Therefore, it would have been obvious to an ordinary skill in the art to design the authentication mechanism accordance with the IEEE 802. lx protocol in order to provide an alternative and robust authentication mechanism.

Regarding claim 4, Tsuchiya et al teaches the network access device wherein the user policy identifies an access control list (Fig 3; Col 2, starts at line 35; authentication unit utilizing control, or authentication table, or host table).

Regarding claim 5, Tsuchiya et al teaches the network access device wherein the user policy includes an access control list (Fig 3; Col 2, starts at line 35; control, or authentication table).

Regarding claim 6, Tsuchiya et al teaches the network access device wherein the user policy identifies a Media Access Control (MAC) address filter (Fig 2; MAC address in host table). Furthermore, Kameda teaches the network access device wherein the user policy identifies a Media Access Control (MAC) address filter (Fig 1.22; MAC address filter in switch table)

Regarding claim 7, Kameda teaches the network access device wherein the user policy includes a Media Access Control (MAC) address filter (Fig 1.22; MAC address filter in switch table).

Regarding claim 8, Kameda teaches the device wherein the control logic is adapted to send user information to an authentication server and to receive an accept message from authentication server if the user information is valid (Fig 1; authentication server; Fig 1.2 and 51; Par 53-54, 60-62; assigning/ filtering ports, MAC addresses according to the authentication database).

Regarding claim 9, Kameda teaches the network access device of claim 8, wherein the authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server (Fig 1; Par 012,037; remote authentication server).

Regarding claim 10, it is rejected applying as above applied rejecting claim 9, furthermore, Kameda teaches the network access device wherein the accept message includes the user policy (Fig 1; authentication server table including authentication response information; Fig 1.2 , 5 and 51; Par 53-54, 60-62; server authentication database) .

Regarding claim 11, Tsuchiya et al teaches the network access device wherein the control logic is further adapted to assign the one of the plurality of input ports to a virtual local area network (VLAN) associated with the user information if the user information is valid (Fig 2; Col 1, starts at line 16; authenticating VLAN information).

Regarding claim 12, Tsuchiya et al teaches the network access device wherein the control logic is adapted to receive a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information, and to assign the one of the plurality of input ports to a VLAN associated with the VLAN ID (Fig 2; Col 1, starts at line 16; authenticating VLAN information/ number).

Regarding claim 44, Tsuchiya et al teaches the device wherein the user information comprises a user name and a password (Fig 3; Col 8, lines 40-50).

Regarding claims 14-22, 24-34 and 45-46, they recite the limitations of claims 1-13, 23 and 44, therefore, they are rejected applying as above applied rejecting claims 1-13, 23 and 44.

9. Claims 35-43 are rejected under 35 U.S.C. 103(a) as obvious over Tsuchiya et al (US 7360086 B1) in view of Kameda (US 2003/0028808 A1) further in view of Volpano (US 7188364 B2)

Regarding claim 35, Tsuchiya et al teaches the network access device of claim 2 wherein the control logic is further configured to:

if authentication of the MAC address indicates the MAC address is invalid,

drop packets from the user device, or disable the port (Col 3, lines 17-45; Col 10, lines 36-67; Col 14, lines 5-55; discarding/ not sending the packets upon authentication with the host table/ MAC address or port number);

if authentication of user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the network access device (Fig 2, Fig 3; Col 10, lines 10-50; Col 14, lines 5-55);

if the user is not associated with the VLAN,

assign the port to a port default VLAN (Fig 2; Col 10, lines 10-50; Col 14, lines 5-55; VLAN, and port assignment);

if the user is associated with the VLAN,

assign the port to the VLAN associated with the user; and forward packets from the user device (Fig 2; Col 10, lines 10-50; Col 14, lines 5-55; VLAN, and port assignment based on user, and VLAN association/ authentication)

Modified Kameda- Tsuchiya et al system fails to disclose expressly if authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol; if the user is not associated with the VLAN, block all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol.

However, Volpano discloses if authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol (Col 5, starting at line 30; control frames; EAPOL); if the user is not associated with the VLAN, block all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol (Col 5, starting at line 30; control frames; EAPOL).

Volpano and Tsuchiya et al are analogous art because they are from the same field of endeavor of VLAN utilizing bridges/ switches. At the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teachings of modified Kameda-Tsuchiya et al device with Volpano to design an apparatus further adapted to drop/ filter packets by authenticating utilizing an authentication server, authentication protocol message containing VLAN identifier in order to provide a proper VLAN packet filtering.

Regarding claim 38, it is rejected applying as above applied rejecting claim 35, furthermore, Tsuchiya et al teaches an apparatus/ method/ system for providing network security, comprising:

a plurality of input ports (Fig 1.21-25; Col 1, starts at line 25; LAN switch with plural ports);

a switching fabric for routing data received on the plurality of input ports to at least one output port (Fig 1; Fig 7.210; LAN switch with the routing, and port information); and

control logic (Col 2, starts at line 35; Col 7, starts at line 5; authentication, or control information) adapted to: authenticate a physical address of a user device coupled to one of the

plurality of input ports (Col 8, starts at line 5; MAC address authentication, association with the specific port);

drop packets from the user device if the physical address is invalid (Col 3, lines 17-45; Col 10, lines 36-67; Col 14, lines 5-55; discarding/ not sending the packets upon authentication with the host table/ MAC address or port number);

authenticate user information provided by a user of the user device only if the physical address is valid (Col 3, lines 17-45; Col 10, lines 10-50; authenticating user with the authentication table after matching of the address/ MAC in host table);

if authentication of user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the apparatus by receiving a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information (Fig 2; Col 1, starts at line 16; authenticating VLAN information/ number);

if the user is associated with the VLAN, assign the one of the plurality of ports to the VLAN associated with the user; and restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information (Col 10, lines 10-50; Col 14, lines 5-55).

Modified Kameda- Tsuchiya et al system fails to disclose expressly if authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol; if the user is not associated with the VLAN, block all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol.

However, Volpano discloses if authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol (Col 5, starting at line 30; control frames; EAPOL); if the user is not associated with the VLAN, block all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol (Col 5, starting at line 30; control frames; EAPOL).

Regarding claim 39, Tsuchiya et al teaches the apparatus wherein the apparatus comprises a layer 2 network access device.

Regarding claims 36-37 and 40-43, they recite the limitations of claims 13, 35 and 38-39, therefore, they are rejected applying as above applied rejecting claims 13, 35 and 38-39.

Conclusion

10. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner. Finally, for any future amendments to claims, the applicant is respectfully requested to incorporate the paragraph numbers from the specification upon which the support for such amendments were obtained.

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 8:30 AM to 6:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. The RightFax number for faxing directly to the examiner is 571-273-3551.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436